P.4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/432,297	11/02/1999	EARL THOMAS CARTER	2705-76	9858

20575 7590 09/15/2003

MARGER JOHNSON & MCCOLLOM PC
1030 SW MORRISON STREET
PORTLAND, OR 97205

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2172	2

DATE MAILED: 09/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PPG

Office Action Summary	Application No.	Applicant(s)	
	09/432,297	CARTER ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf (US 6, 301, 668 B1), and further in view of Blanchard (US 6, 219, 791 B1).

a. *Referring to claims 1 and 14:*

i. Gleichauf teaches:

(1) storing the plurality of encrypted query data packets in a memory **[i.e., data stored in memory or fixed storage on the workstation or other device in which network security system resides (column 5, line 19-21)]** ; and thereafter

(2) scanning the networked computer for a target vulnerability residing therein by sending successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature **[i.e., Figure 2, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42)].**

ii. However Gleichauf does not teach:

(1) encrypting a query data packet in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability;

iii. Whereas Blanchard teaches:

(1) Figure 1, encryptor 20 includes key generator 24 and exclusive-or (XOR) 22, which receives plain text on signal 15, and receives key 25 from key generator 24. XOR 22 applies key 25 to the plain text to generate encrypted data packets on signal 26.

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such encryptor (such as Figure 2 of Gleichauf) in order to encrypt data packets and compare, and if they do not match, then an error has been detected, and transmission can be stopped **(column 1, line 17-20 of Blanchard).**

v. The ordinary skilled person would have been motivated to:

(1) add such encryptor (such as Figure 2 of Gleichauf) because many communications systems benefit from secure communications provided by encrypted digital data packets **(column 1, line 13-15).**

b. *Referring to claim 2:*

i. Gleichauf further teaches:

(1) in which plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural networked computers and by analyzing responses thereto from each of the plural networked computers **[i.e., Figure 2, scan engine 22 scans devices on internal network, such as workstations 12. It also analyzes the network information to identify potential vulnerabilities of internal network and can direct requests upon the network and assess responses to such requests to discover network information (column 5, line 52-65)].**

c. *Referring to claim 3:*

i. Gleichauf further teaches:

(1) in which plural ports of plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural ports of each of plural networked computers and by analyzing responses thereto from each of the plural ports of each of the plural networked computers **[i.e., can include port scans (column 4, line 1)]**.

d. *Referring to claim 4:*

i. Gleichauf further teaches:

(1) wherein the target vulnerability is Trojan Horse software residing in a port of the networked computer **[i.e., a signature engine is coupled to the network and compares the network data traffic to a plurality of attack signatures to identify attacks upon the network, and each of the attack signatures are designed to detect a particular type of attack upon the network (column 2, line 63-65 and column 8, line 40-42)]**.

e. *Referring to claim 5:*

i. This claim has limitations that are similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

f. *Referring to claim 6:*

i. Blanchard further teaches:

(1) wherein said encrypting is performed for substantially all of the encryption keys within a defined key space **[i.e., Figure 2, trusted key generator 105 provides key 11 to encryptor 21, and provides key 120 o decryptor 31. The use of a trusted key generator is advantageous in part because trusted key generators are commercially available and have undergone independent certification (column 3, line 39-44)]**.

g. *Referring to claims 7 and 8:*

i. Gleichauf does not explicitly teaches:

(1) wherein said storing is to a non-volatile memory.

(2) writing the stored plurality of encrypted query data packets from the non-volatile memory to a cache memory prior to said scanning.

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) identify those specific kinds of memory (such as Figure 2, storage 36 of Gleichauf) in order to maintain the storing data when the power is lost and since virus checking can be a resource-intensive operation, check files and/or results of checks may be advantageously stored in a cache memory.

iii. The ordinary skilled person would have been motivated to:

(1) clarify these type of memory reside within the storage (such as Figure 2, storage 36 of Gleichauf) because it is a common practice to store data in these type of memory which are well known in the art.

h. *Referring to claim 9:*

i. Gleichauf teaches:

(1) a memory device for storing the database **[i.e., Figure 2, storage 36 comprise memory or fixed storage (column 5, line 21-22)]**;

(2) a transmitter for transmitting said database to a plurality of computers connected with a network **[i.e., Figure 2, scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (column 5, line 52-54)]**; and

(3) an analyzer for analyzing responses from the plurality of computers to said transmitting, said analyzer recognizing and recording one or more signature responses along with one or more corresponding addresses of the one or more signature-respondent computers **[i.e., Figure 2, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42)]**.

ii. However Gleichauf does not teach:

(1) a pre-processor for encrypting a query data packet in accordance with a plurality of different keys and storing a plurality of such differently encrypted query data packets in a database, the query data packet including one or more fields of data to which a Trojan Horse if resident in a given computer would make a signature response;

iii. Whereas Blanchard teaches:

(1) Figure 3, show a data encryption and verification system which includes a processor 310, memory 360, processor 330, and memory 380. A second portion of memory 380, portion 384, includes commands for processor 330 to perform error detection and to generate signal 350 **(column 3, line 45-48 and column 4, line 35-38).**

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such processor (such as Figure 2 of Gleichauf) in order to encrypt data packets and compare, and if they do not match, then an error has been detected, and transmission can be stopped **(column 1, line 17-20 of Blanchard).**

v. The ordinary skilled person would have been motivated to:

(1) add such processor (such as Figure 2 of Gleichauf) because many communications systems benefit from secure communications provided by encrypted digital data packets **(column 1, line 13-15).**

i. *Referring to claims 10, 11, 12, 15, 16, and 17:*

i. These claims have limitations that are similar to those of claims 7 and 8, thus it is rejected with the same rationale applied against claims 7 and 8 above.

j. *Referring to claims 13, 18, and 19:*

i. These claims have limitations that are similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Tso et al, US 6, 088, 803 discloses a system for virus checking a data object to be downloaded to a client device. Upon retrieval of a data object to be downloaded, the data object is scanned for a computer virus. If no computer virus is detected, the data object is downloaded to the client device (column 1, line 57-62).

b. Feiken, US 5,870,479 discloses a device for processing data packets, comprising identification means for identifying a data packet, processing means for cryptographically processing the data packet, and memory means for storing information relating to the processing (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
September 8, 2003

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100